Секция «Дискретная математика и математическая кибернетика»

Критерий надежности канала с запрещениями и его применение к блужданиям по плоскости.

Научный руководитель – Галатенко Алексей Владимирович

Казаков Илья Борисович
Студент (специалист)
Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра математической теории интеллектуальных систем, Москва, Россия
E-mail: i_b_kazakov@mail.ru

Скрытым каналом называется коммуникационный канал, пересылающий информацию методом, который изначально не был для этого предназначен. Это означает, что существуют злоумышленники, передающие информацию таким образом, что сторонние наблюдатели не могут зафиксировать сам факт передачи. Исторически первой работой, посвященной теории скрытых каналов, считается статья [1]. Для примера, укажем также более современый обзор [2], посвященный сетевым скрытым каналам.

Конкретно в данном докладе, речь пойдет о скрытом канале блужданий по плоскости. Блуждания по плоскости изучаются в связи с задачей построения скрытых каналов через online-шутеры, то есть многопользовательские игры, в которых некий клиент может передавать игровому серверу команды о перемещении своего персонажа по плоскости, а другие клиенты могут получать от сервера данные о местоположении данного персонажа. Задача построения таких каналов исследовалась, например, в [3]. Однако, в [3] не ставился вопрос о передаче информации в условиях, когда движение игрока-передатчика по плоскости может быть произвольным образом ограничено.

Протокол передачи данных через блуждания по плоскости задан следующим образом. Вся игровая плоскость разбита на многоугольники. Актом передачи информации считается пересечение границы многоугольника (в котором в данный момент находится передающий игрок) в одном из возможных направлений.

Однако, в реальных online-играх движение персонажей по игровому полю не является абсолютно свободным. Этому имеются многообразные причины. Во-первых, игровое поле имеет границы, и, стало быть, игрок-передатчик не может находиться за их пределами. Во-вторых, игрок-приемник может иметь ограниченную область видимости, за пределы которой, следовательно, игроку-передатчику не следует выходить. В-третьих, на карте имеются естественные препятствия, вроде «камней», «воды» и т.д, то есть зоны, где игроки не могут находиться.

То есть может оказаться так, что по некоторым направлениям игроку-передатчику ходить нельзя, то есть невозможно передать некоторые из возможных значений. При этом игрок-приемник может как знать, какие именно направления сейчас запрещены, так и не знать, куда же игрок-передатчик «не хочет идти».

И следовательно, возникает задача конструирования схемы кодирования информации для передачи в вышеописанных условиях. Сведём задачу к следующей абстрактной постановке: пусть дан алфавит из n символов, и пусть на каждом шаге может быть запрещено (неким третьим субъектом, называемым традиционно Евой) не более, чем $n-k$ из них. При каких n и k возможно гарантированно передать заданный символ? Таким образом определённый абстрактный канал передачи называется каналом с запрещениями.

Теорема 1. *Канал с запрещениями надежен, т.е. гарантированно передавать по нему информацию возможно тогда и только тогда, когда выполнено условие* $n > 2k - 2$

В случае, если запрещения меняются не чаще, чем один раз в два такта, надежный канал с запрещениями существует тогда и только тогда когда $n - k > 1$.

На автоматном языке возможна следующая интерпретация результата. Рассмотрим следующую игру. Игрок А строит конечный автомат с n-буквенным входным автоматом и выделяет два непересекающихся подмножества состояний Q_0 и Q_1. Игрок Е выбирает значение $a \in \{0, 1\}$ и на каждом такте запрещает не более k входных символов. Задача игрока А привести атомат в состояние Q_a, не попадая в состояния $Q_{\bar{a}}$. Тогда выигрышная стратегия у А существует тогда и только тогда, когда $n > 2k - 2$.

Источники и литература

1) B. W. Lampson. A Note on the Confinement Problem. Communications of the ACM, 16(10):613–615, oct 1973.
2) D. Llamas, AHD Miller, C. Allison. Covert channels in internet protocols: a survey. In Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, PGNET. 2005
3) S. Zander, G. Armitage, P. Branch, Proc. 33rd IEEE Conf. LCN, pp. 215-222, Oct. 2008.